



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/098,575	03/18/2002	Hisashi Nakagomi	220944US2	3219
22850	7590	12/11/2007	EXAMINER	
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			PAN, JOSEPH T	
		ART UNIT	PAPER NUMBER	
		2135		
		NOTIFICATION DATE	DELIVERY MODE	
		12/11/2007	ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/098,575	NAKAGOMI ET AL.	
	Examiner Joseph Pan	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 September 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-22 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-22 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 18 March 2002 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____.	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

1. Applicant's response filed on September 17, 2007 has been carefully considered. Claims 1, 5, 7, 10, 13, 15, 17 and 21 have been amended. Claims 1-22 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-4, 6-11, and 14-20, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono et al. (U.S. Patent No. 6,496,930 B1), hereinafter "Ono", in view of Yoshizawa (U.S. Patent No. 6,928,166 B2).

Referring to claim 1:

i. Ono teaches:

A mobile communication terminal device configured to communicate with a remote device via a wireless connection, the remote device configured to operate at one of a plurality of communication link security levels (see

figure 1, element 2, 'client apparatus'; and column 7, lines 39-44 '...a radio or cable channel...', of Ono), comprising:

a detection unit configured to detect which of the plurality of communication link security levels is in use at the remote device (see fig. 7, element S206 'which conversion type is specified?'; column 12, lines 28-55; and column 3, lines 17-21 '...which encryption/digital signature method should be used,...', of Ono); and

an announcing unit configured to announce said detected communication link security level, each of said plurality of communication security link levels corresponding to a strength of ciphering in use at the remote device (see figure 1, element 221 'input/output controlling unit'; and column 3, lines 17-21 of Ono).

Ono discloses detecting which of the plurality of communication link security levels [i.e., encryption, digital signature, encryption and digital signature, etc., see figure 7 of Ono] is in use at the remote device. However, Ono does not explicitly mention the term "security level".

ii. Yoshizawa teaches a radio communication device and user authentication method, wherein Yoshizawa discloses "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (see column 2, lines 62-64 of Yoshizawa).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels, because Ono teaches a security communication method (see column 1, lines 11-14 of Ono), wherein the security level used in the remote device can be detected from the 'encryption variable' in the input message (see figure 6, 'encryption variable' of Ono). And Yoshizawa teaches "selecting a security level from a plurality of security levels in accordance with a condition of the

radio communication" (emphasis added). Therefore, Yoshizawa's teaching could enhance Ono's system.

Referring to claim 2:

Ono and Yoshizawa teach the claimed subject matter: a mobile communication terminal device configured to communicate with a remote device via a wireless connection (see claim 1 above). Ono further discloses a judgment unit (see column 8, lines 65-column 9, line 8 of Ono).

Referring to claim 3:

Ono and Yoshizawa teach the claimed subject matter: a mobile communication terminal device configured to communicate with a remote device via a wireless connection (see claim 1 above). Ono further discloses the communication link security level setting unit (see column 3, lines 17-21 'Accordingly, the message receiving apparatus can specify...which encryption/digital signature method should be used,', of Ono).

Referring to claim 4:

Ono and Yoshizawa teach the claimed subject matter: a mobile communication terminal device configured to communicate with a remote device via a wireless connection (see claim 1 above). Ono further discloses the control unit (see figure 1, element 21 'encryption/communication control unit' of Ono).

Referring to claims 6, 14, 22:

Ono and Yoshizawa teach the claimed subject matter: a mobile communication terminal device configured to communicate with a remote device via a wireless connection (see claim 1 above). Ono further discloses the notification (see column 11, lines 33-37 of Ono).

Referring to claim 7:

- i. Ono teaches:

A server device configured to communicate with a mobile communication terminal device at a remote location via a wireless telecommunications network and in accordance with one of a plurality of communication link security levels

(see figure 1, element 4 'server apparatus'; and column 7, lines 39-44 '...a radio or cable channel...', of Ono), comprising:

a server side detection unit configured to detect which of the plurality of communication link security levels is being used by said mobile communication terminal (see figure 8 'control procedure of server apparatus', element S254 'which conversion type' of Ono); and

a server side communication link security level setting unit configured to set at least one of a communication link security level permitting communication and a communication link security level not permitting communication, each corresponding to said communication link security level being used by said mobile communication terminal (see e.g. column 1, lines 32-42 of Ono),

wherein said server device is configured to communicate with said mobile communications terminal, each of said plurality of communication link security levels corresponding to a strength of ciphering in use at the remote device (see e.g. column 1, lines 32-42 of Ono).

Ono discloses detecting which of the plurality of communication link security levels [i.e., encryption, digital signature, encryption and digital signature, etc., see figure 7 of Ono] is in use at the mobile communication terminal. However, Ono does not explicitly mention the term "security level".

ii. Yoshizawa teaches a radio communication device and user authentication method, wherein Yoshizawa discloses "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (see column 2, lines 62-64 of Yoshizawa).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels, because Ono teaches a security

communication method (see column 1, lines 11-14 of Ono), wherein the security level used in the remote device can be detected from the 'encryption variable' in the input message (see figure 6, 'encryption variable' of Ono). And Yoshizawa teaches "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (emphasis added). Therefore, Yoshizawa's teaching could enhance Ono's system.

Referring to claim 8:

Ono and Yoshizawa teach the claimed subject matter: a server device configured to communicate with a mobile communication terminal device (see claim 7 above). Ono further discloses the control unit (see figure 1, element 41 'encryption/communication control unit' of Ono).

Referring to claims 9, 16:

Ono and Yoshizawa teach the claimed subject matter: a server device configured to communicate with a mobile communication terminal device (see claim 7 above). Ono further discloses the inquiry unit (see column 2, lines 9-17 of Ono).

Referring to claim 10:

i. Ono teaches:

A mobile communication terminal device having a security communication function, comprising:

(a) a detection unit configured to detect which of the plurality of communication link security levels is in use at the remote device (see figure 7, element S206 'which conversion type is specified?'; and column 12, lines 28-55, of Ono);

(b) an announcing unit configured to announce said detected communication link security level (see figure 1, element 32 'input/output controlling unit' of Ono);

(c) a communication link security level setting unit configured to set by a user at least one of a communication link security level permitting communication and a communication link security level not permitting communication (see column 3, lines 17-21 '...specify...which encryption/digital signature method should be used,' of

Ono);

(d) an internal memory configured to store the communication link security level information set by the user via the communication link security level setting unit (see figure 1, element 2 'client apparatus' of Ono);

(e) a judgment unit configured to judge whether said detected level satisfies the communication link security level condition previously set by the user (see column 8, line 65-column 9, line 8 of Ono); and

(f) a control unit configured to prevent the establishment of communications when the communication link security level condition is not satisfied or allow communication when the communication link security level condition is satisfied, each of said plurality of communication link security levels corresponding to a strength of ciphering in use at the remote device (see column 1, lines 32-42; and figure 7, element S206 'which conversion type is specified?' of Ono).

Ono discloses detecting which of the plurality of communication link security levels [i.e., encryption, digital signature, encryption and digital signature, etc., see figure 7 of Ono] is in use at the remote device. However, Ono does not explicitly mention the term "security level".

ii. Yoshizawa teaches a radio communication device and user authentication method, wherein Yoshizawa discloses "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (see column 2, lines 62-64 of Yoshizawa).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels, because Ono teaches a security communication method (see column 1, lines 11-14 of Ono), wherein the security level used in the remote device can be detected from the 'encryption variable' in the input

message (see figure 6, 'encryption variable' of Ono). And Yoshizawa teaches "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (emphasis added). Therefore, Yoshizawa's teaching could enhance Ono's system.

Referring to claim 11:

Ono and Yoshizawa teach the claimed subject matter: a mobile communication terminal device (see claim 10 above). Ono further discloses the accounting unit (see figure 1, element 22 'input/output controlling unit' of Ono).

Referring to claim 15:

i. Ono teaches:

A server device configured to communicate with a mobile communication terminal device via a communication network and via one of a plurality of communication link security levels, the server device comprising:

(a) a server side detection unit, configured to detect which of the plurality of communication link security levels are in use in the mobile communication terminal device (see figure 8, element S254 'which conversion type?' of Ono);

(b) a server side communication link security level setting unit configured to set by a user at least one of a communication link security level permitting communication and a communication link security level not permitting communication, wherein the server side communication link security level setting unit is configured to be set by a user, and the server device also comprises (see column 1, lines 32-42 of Ono):

(c) an internal memory configured to store the communication link security level information set by the user via the server side communication link security level setting unit (see figure 1, element 41 'encryption/communication control unit' of Ono);

(d) a server side control unit configured to prevent communication when said detected communication link security level has not reached said communication link security level permitting communication or to discontinue communication when said detected communication link security level falls below said

communication link security level not permitting communication, each of said plurality of communication link security levels corresponding to a strength of ciphering in use at the remote device (see figure 1, element 41 'encryption/communication controlling unit'; and column 1, lines 32-42 of Ono).

Ono discloses detecting which of the plurality of communication link security levels [i.e., encryption, digital signature, encryption and digital signature, etc., see figure 7 of Ono] is in use at the mobile communication terminal device. However, Ono does not explicitly mention the term "security level".

ii. Yoshizawa teaches a radio communication device and user authentication method, wherein Yoshizawa discloses "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (see column 2, lines 62-64 of Yoshizawa).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels, because Ono teaches a security communication method (see column 1, lines 11-14 of Ono), wherein the security level used in the remote device can be detected from the 'encryption variable' in the input message (see figure 6, 'encryption variable' of Ono). And Yoshizawa teaches "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (emphasis added). Therefore, Yoshizawa's teaching could enhance Ono's system.

Referring to claim 17:

i. Ono teaches:

A method of communicating between a mobile communication terminal device and a remote device via a wireless connection, the remote device configured to operate at one of a plurality of communication link security levels,

comprising:

detecting which of the plurality of communication link security levels is in use at the remote device (see figure 8, element S254 'which conversion type?'; and column 12, lines 28-55, of Ono); and

announcing said detected communication link security level, each of said plurality of communication link security levels corresponding to a strength of ciphering in use at the remote device (see figure 1, element 4 'server apparatus' of Ono).

Ono discloses detecting which of the plurality of communication link security levels [i.e., encryption, digital signature, encryption and digital signature, etc., see figure 7 of Ono] is in use at the remote device. However, Ono does not explicitly mention the term "security level".

ii. Yoshizawa teaches a radio communication device and user authentication method, wherein Yoshizawa discloses "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (see column 2, lines 62-64 of Yoshizawa).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yoshizawa into the system of Ono to allow selecting a security level amount a plurality of security levels, because Ono teaches a security communication method (see column 1, lines 11-14 of Ono), wherein the security level used in the remote device can be detected from the 'encryption variable' in the input message (see figure 6, 'encryption variable' of Ono). And Yoshizawa teaches "selecting a security level from a plurality of security levels in accordance with a condition of the radio communication" (emphasis added). Therefore, Yoshizawa's teaching could enhance Ono's system.

Referring to claim 18:

Ono teaches the claimed subject matter: a method of communicating between a mobile communication terminal device and a remote device via a wireless connection (see claim 17 above). Ono further discloses the judging unit (see figure 8, element S254 'which conversion type?' of Ono).

Referring to claim 19:

Ono and Yoshizawa teach the claimed subject matter: a method of communicating between a mobile communication terminal device and a remote device via a wireless connection (see claim 17 above). Ono further discloses the setting (see column 3, lines 17-21 '...specify...which encryption/digital signature method should be used,' of Ono).

Referring to claim 20:

Ono and Yoshizawa teach the claimed subject matter: a method of communicating between a mobile communication terminal device and a remote device via a wireless connection (see claim 17 above). Ono further discloses the establishment or preventing the establishment of communications between a mobile communication terminal device and a remote device (see column 1, lines 32-42 of Ono).

4. Claims 5, 12-13 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono et al. (U.S. Patent No. 6,496,930 B1) in view of Yoshizawa (U.S. Patent No. 6,928,166 B2), and further in view of Tanaka et al. (U.S. Patent No. 6,208,376 B1), hereinafter "Tanaka".

Referring to claims 5, 12-13, 21:

i. Ono and Yoshizawa teaches the claimed subject matter: a mobile communication terminal device configured to communicate with a remote device via a wireless connection (see claim 1 above). Ono further discloses urging the user to input

a message (see column 2, lines 9-17 of Ono). However, they do not specifically mention urging the selection of the continuance or discontinuance of communication.

ii. Tanaka teaches a communication system and method wherein Tanaka discloses urging a user to select either to "continue" or "stop" when a warning is issued (see column 6, lines 12-15 of Tanaka).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Tanaka into the system of Ono and Yoshizawa to urge a user to select either to "continue" or "stop" when a warning is issued.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Tanaka into the system of Ono and Yoshizawa to urge a user to select either to "continue" or "stop" when a warning is issued, because Ono and Yoshizawa teach a security communication method (see column 1, lines 11-14 of Ono), and the terminal device analyze the encryption variable in the input message (see figure 7, element S206 'Analyze encryption variable' of Ono). It would enhance the system of Ono and Yoshizawa by urging a user to select either continue or stop when the encryption variable changes during the data communication.

Response to Arguments

5. Applicant's arguments filed on September 17, 2007, have been fully considered but they are not persuasive.

Applicant argues:

"However, Ono does not disclose or suggest Applicants' claimed detection unit configured to detect which of the plurality of communication link security levels is in use

at the remote device as said preset communication link security level, as recited in Applicants' amended Claim 1." (see page 3, 4th paragraph)

Examiner maintains:

Ono discloses "When the user inputs a message (plaintext 313 in FIG. 5) on the message input form, the encryption variable in the message input form creation document 312 is analyzed (S205) to specify a conversion type (S206) [i.e., "detecting which of the plurality of communication security levels is in use at the remote device as said preset communication link security level"]. When the encryption variable is "ONLY", the input message is encrypted using the specified encryption method (RSA in FIG. 6) (S207). When the encryption variable is "MIC-CLEAR", the input message is digitally signed using the specified digital signature method (public key cryptosystem) (S208). When the encryption variable is "ENCRYPTED", the input message is encrypted and digitally signed using the specified encryption method (MyElIty-DES-CBC) and digital signature method (MyElIty-SHA-1) (S209).

After encrypting and/or digitally signing the input message according to the conversion type specified by the encryption variable, the client apparatus 2 transmits the converted message to the server apparatus 4 as the communication text 314 (S210) and waits for the communication completion notification 316 as the reply to the communication text 314 (S211). If, on the other hand, the message input form creation document 312 does not include an encryption variable in step S205, the client apparatus 2 judges that neither encryption nor digital signature is necessary and transmits the input message directly to the server apparatus 4 as the communication text 314 in step S210. On receiving the communication completion notification 316 from the server apparatus 4, the client apparatus 2 completes the procedure." (see column 12, lines 28-55 of Ono, emphasis added).

Therefore, Ono discloses the claimed detection unit configured to detect which of the plurality of communication link security levels is in use at the remote device as said preset communication link security level, as recited in Applicants' amended Claim 1.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office Action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

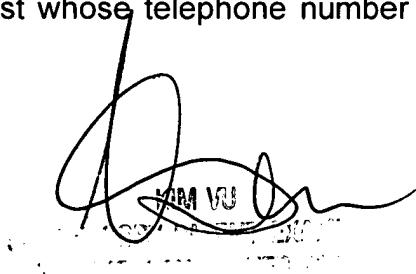
The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan



JOSEPH PAN
KIM VU
EXAMINER
ART UNIT 2135
TELEPHONE 571-272-5987
FAX 571-273-8300